IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION

UNITED STATES OF AMERICA	§	
	§	
v.	§	No. 3:09-CR-210-B
	§	
JESSE WILLIAM MCGRAW (1)	§	
also known as Ghost Exodus	§	

FACTUAL RESUME

Jesse William McGraw, John Nicholson, the defendant's attorney, and the United States of America (the government), agree that the following accurately states the elements of the offense and the facts relevant to the offense to which the defendant is pleading guilty:

Elements:

1. In order for the defendant to be convicted at trial of a violation of 18 U.S.C. §1030(a)(5)(A) and §1030(c)(4)(B)(i)(II) (and in Count Two §1030(c)(4)(B)(i)(IV)), the United States would have to prove each of the following elements of the offense beyond a reasonable doubt:

First: That McGraw, through means of a computer used in interstate commerce or communications, knowingly caused the transmission of a program, information, code, or command to another computer or computer system, as charged;

Second: That McGraw, by causing the transmission intended to damage the receiving computer, computer system, information, data or program, and withhold or deny, or cause the withholding or denial, of the use of a computer, computer services, system, or network, information, data or program;

Third: That McGraw so acted without the authorization of the persons or entities who own or are responsible for the computer system receiving the program, information, code, or command; and

Fourth: That McGraw's acts potentially modified or impaired, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals; *and*

for Count Two
Fifth: *That McGraw's acts potentially created a risk to public health and safety.*

Facts:

1. From October 30, 2008, until June 26, 2009, McGraw was employed as a security guard for United Protection Services, a security firm in Dallas, Texas. From November 1, 2008, until June 26, 2009, McGraw was assigned by United Protection Services to work security at the North Central Medical Plaza, located at 9301 North Central Expressway, Dallas, Texas. The North Central Medical Plaza housed medical offices and surgery centers, to include the W.B. Carrell Memorial Clinic[1] and the North Central Surgery

[1] The W. B. Carrell Memorial Clinic provides comprehensive orthopaedic care by board certified orthopaedic surgeons and staff.

Center[2]. Generally, McGraw's shift was Thursday through Tuesday, from 23:00[3] until 07:00. McGraw's assignment constituted a position of trust.

2. The following computers (or computer systems) were located within the North Central Medical Plaza, and constituted protected computers pursuant to 18 U.S.C. §1030(e)(2), in that they were used in or affecting interstate commerce or communications.

a. The Nurses Station E computer had the host name WBCCW125 and was located on the 5th floor of the North Central Medical Plaza. The computer was used to track a patients progress through the W.B. Carrell Memorial Clinic. Medical staff also used the computer to reference a patient's personal identifiers, billing records, and medical history.

b. The HVAC computer was located in a locked room of the North Central Medical Plaza and was used by the building engineering staff. The HVAC computer was used to control the Heating Ventilation and Air Conditioning for the first and second floors used by the North Central Surgery Center.

3. McGraw gained physical access to approximately 14 computers located in the North Central Medical Plaza, including the two identified above. McGraw does not have specific recollection of installing (transmitting) "Logmein," an application program that

[2] The NCSC provides state-of-the-art equipment for surgeons to perform procedures in the speciality areas of General Surgery; Gastroenterology (GI); Gynecology; Ophthalmology; Orthopedic; Pain Management; Plastic Surgery; Podiatry; Ear, Nose and Throat; Bariatric; Spine; and Urology.

[3] All time will be referenced in military time.

allows remote access to computers, to all of the computers that he physically accessed. However, McGraw does have specific recollection of transmitting Logmein to some of the computers and does not contest that he transmitted Logmein to the remainder. The Logmein installation was unauthorized and compromised the integrity of the computer systems and the associated network by allowing unauthorized, remote access by McGraw and anyone with access to his Logmein account name and password. McGraw also impaired the integrity of some, but not all, of the computer systems by removing security features, e.g. uninstalling anti-virus programs, which made the computer systems and related network more vulnerable to attack. McGraw also installed a malicious code and program (sometimes called a "bot") on some, but not all, of the computers. "Bots" are usually associated with theft of data from the compromised computer, using the compromised computer in denial of service attacks, and using the compromised computer to send spam. In this case, McGraw intended to use the "bot" to launch a denial of service attack on the website of a rival "hacker" group. McGraw installed the "bot" known as "RxBot" on some of the compromised computers and controlled the compromised computers from an IRC terminal under his control, specifically the servers eta.myvnc.com and eta2.myvnc.com.

4. McGraw intended to impair the integrity of the accessability of the computers and computer systems, by turning off the security protocols, and by creating a means by which he could remotely access the computers and computer systems. Therefore, by installing (transmitting) the Logmein program and the RxBot program, McGraw damaged and

intended to damage the computers or computer systems as defined by 18 U.S.C. §1030(e)(8).

5. McGraw knew these actions would damage[4] the security of and integrity of these systems. McGraw advocated taking these kinds of actions in order to adversely affect the integrity of systems in instructions that he posted online for members of his "Electronik Tribulation Army" (ETA) and other individuals interested in committing crime against computers.

6. On or about February 12, 2009, McGraw abused the trust placed in him as a security guard and bypassed the physical security to the room in the North Central Medical Plaza containing the HVAC computer. At approximately 23:35, McGraw without authorization began the download (transmission) of "Ophcrack-vista-livecd-2.1.0.iso," a password recovery tool from the website sourcefourge.net. Ophcrack has both lawful and malicious applications. McGraw used Ophcrack in a malicious manner to recover passwords from some, but not all, of the compromised computers. McGraw does not specifically recall that he also used the HVAC computer to download and then install (transmit) without authorization Team Viewer 4, a remote access program. However, McGraw does not contest that he did so. McGraw does not specifically recall circumventing the security software McAfee and adding Teamviewer to the list of allowed programs in McAffee. However, McGraw does

[4] "Damage" is defined in 18 U.S.C. §1030(e)(8) as "any impairment to the integrity or availability of data, a program, a system, or information."

not contest that he did so. By February 13, 2009, at approximately 01:19 McGraw again without authorization physically accessed the HVAC computer and inserted a removeable storage device named "HARD DISK X" and executed the program daemon4301-lite.exe which allowed McGraw to emulate a CD/DVD device with the removeable storage device. McGraw used "Sonic Record Now," a CD/DVD burning software, to create a bootable CD image using a previously downloaded "OphCrack-xp-livecd.iso".

7. On or about April 28, 2009, at about 01:47, McGraw abused the trust placed in him as a security guard and accessed without authorization the Nurses Station E computer. In a video created and narrated by McGraw, McGraw appears to insert into the computer a CD containing the OphCrack program to bypass any passwords or security. McGraw also appears to insert a removeable storage device into the computer which he claimed contained a malicious program or code, called RxBot. FBI found the CD containing the OphCrack program in McGraw's house and found the source code for the RxBot on McGraw's laptop. The application log shows that at the time the video was created, McGraw did disengage the McAfee VirusScan Enterprise program on the computer, which turned off the existing security features making the computer more vulnerable to attack.

8. On or about April 7, 2009, at approximately 02:30, McGraw abused the trust placed in him as a security guard and bypassed the physical security to the room in the North Central Medical Plaza containing the HVAC computer. The application log shows

that, at approximately 03:12, McGraw installed (transmitted) Logmein to the HVAC computer. Although McGraw does not have specific recollection of successfully transmitting Logmein to the HVAC computer, he does have specific recollection of attempting to do so and does not contest that it was successfully done. Furthermore, McGraw admits that he did use his Logmein account to gain unauthorized, remote access to the HVAC computer.

9. On or about the following dates, McGraw remotely accessed without authorization the HVAC computer:

DATE	TIME	DURATION
04/13/09	07:21	5m:43s
04/13/09	07:24	2m:37s
04/13/09	20:09	55m:31s
04/14/09	06:50	2m:38s
04/14/09	06:56	14m:15s

10. McGraw was not authorized, and knew that he was not authorized, to physically or remotely access any of these computers or computer systems located within the North Central Medical Plaza. McGraw was not authorized, and knew that he was not authorized, to transmit any programs, codes, or command to these computers or computer systems.

11. McGraw was aware that some of the computers he compromised, such as the Nurses Station E computer, were used to access and review medical records. McGraw

claims that he did not review or modify patient medical records and the government is not aware of any evidence to the contrary. However, by gaining administrator access to these computers, McGraw would have had the ability to modify these records if he took additional steps such as circumventing additional security measures.

12. McGraw was aware that the HVAC computers were used to maintain the environmental controls at the facility. While McGraw claims that did not plan to adversely affect the actual climate in the facility or harm any of the facility's patients or employees, he knew that by modifying the HVAC computer controls he could affect the temperature of the facility. By affecting the environmental controls of the facility, he could have affected the treatment and recovery of patients who were vulnerable to changes in the environment. In addition, he could have affected treatment regimes, including the efficacy of any or all of the temperature sensitive drugs.

13. McGraw understands that the cost to remediate the compromised computers and computer systems with the North Central Medical Plaza exceeded $30,000, but was less than $70,000.

JAMES T. JACKS
UNITED STATES ATTORNEY

1-29-2010

CANDINA S. HEATH
Assistant United States Attorney
Texas State Bar No. 09347450
1100 Commerce Street, Third Floor
Dallas, Texas 75242-1699
Tel: 214.659.8600
Fax: 214.767.2846
candina.heath@usdoj.gov

Date

I have read (or had read to me) this Factual Resume and have carefully reviewed every part of it with my attorney. I fully understand it and I swear that the facts contained herein are true and correct.

Jesse McGraw

JESSE WILLIAM MCGRAW
Defendant

1-29-10

Date

I am the defendant's counsel. I have carefully reviewed every part of this Factual Resume with the defendant. To my knowledge and belief, my client's decision execute this Factual Resume is an informed and voluntary one.

John M-Nicholson

JOHN NICHOLSON
Attorney for Defendant

1-29-10

Date